

WE CLAIM:

1. A method of updating a system BIOS, comprising:
receiving a data object having a BIOS package and an associated signature,
authenticating the BIOS package using a public key stored on the computer and
the signature, and
if the authentication succeeds, writing the BIOS package to firmware on the
computer system.
2. The method of claim 1, wherein the signature is generated by a public key-private
key pair, the public key of which is stored on the computer.
3. The method of claim 1, wherein the receiving comprises loading the data object
from a storage device.
4. The method of claim 1, wherein the receiving comprises receiving the data object
from a communication network.
5. The method of claim 1, wherein the receiving comprises receiving the data object
from a computer network.
6. The method of claim 1, further comprising, prior to the writing:
via an operating system, storing fragments of the received data object in system
memory,
creating a table identifying locations of each fragment in system memory, and
assembling the BIOS package from the fragments using the table.
7. A method for updating a system BIOS for a processor, comprising, upon restart of
the processor:
determining whether system memory contains a BIOS package,
authenticating the BIOS package, and
upon successful authentication, storing the BIOS package in firmware.
8. The method of claim 7, further comprising:
determining whether the BIOS package is successfully stored in the firmware,

if so, report a success flag identifying the BIOS package as successfully stored.

9. A computer system, comprising:

a processor,

firmware electrically connected to the processor, the firmware comprising:

a first storage space to store a first system BIOS, the first storage space being a read only memory,

a second storage space to store a second system BIOS and an index table associating elements of the second system BIOS with elements of the first system BIOS.

10. The computer system of claim 9, wherein the first storage space is to store a system BIOS and at least one ancillary BIOS and the index table identifying the BIOSs.

11. A method of publishing updates for system BIOSs of deployed computer systems, comprising:

based on content of the BIOS update, creating a digital signature according to a private key of a public key-private key pair,

storing the BIOS update and the digital signature on a storage medium, responsive to a request from a computer, transferring the BIOS update and the digital signature to the computer.

12. The method of claim 10, wherein the transferring comprises transferring the data object from a memory device.

13. The method of claim 10, wherein the transferring comprises transferring the data object from a communication network.

14. The method of claim 10, wherein the transferring comprises transferring the data object from a computer network.

15. The method of claim 10, wherein a public key of the public key-private key pair is stored in the computer.

16. A BIOS processing method, comprising:
executing a system BIOS from a default memory space,

executing an ancillary BIOS according to:

determining whether an ancillary BIOS exists in an alterable memory space,

if no ancillary BIOS exist in the alterable section, executing an ancillary BIOS from the default memory space.

17. The method of claim 16, further comprising, if an ancillary BIOS exists in the alterable section, executing the ancillary BIOS in the alterable section.

18. The method of claim 16, further comprising, determining whether a predetermined user command has been entered and, if no predetermined user command has been entered, executing the ancillary BIOS from the alterable section.

19. The method of claim 16, further comprising:
decompressing an ancillary BIOS from the alterable section and
executing the decompressed ancillary BIOS.

20. An ancillary BIOS processing method, comprising:
determining whether an ancillary BIOS package is present in an enhancement space of firmware,
if the ancillary BIOS package is present, determining whether a predetermined user command has been entered,
if the predetermined user command has not been entered, executing the ancillary BIOS package from the enhancement space,
otherwise, executing an ancillary BIOS from a default space of firmware.

21. The method of claim 20, further comprising:
decompressing the ancillary BIOS from the alterable section and
executing the decompressed ancillary BIOS.

22. An ancillary BIOS processing method, comprising:
determining whether an ancillary BIOS package is present in an enhancement space of firmware,
if the ancillary BIOS package is present, determining whether a predetermined flag has been set in the firmware,

if the predetermined user command has been set, executing the ancillary BIOS package from the enhancement space,
otherwise, executing an ancillary BIOS from a default space of firmware.

23. The method of claim 22, further comprising:

decompressing an ancillary BIOS from the alterable section and
executing the decompressed ancillary BIOS.

24. An ancillary BIOS processing method, comprising:

determining whether an ancillary BIOS package is present in an enhancement space of firmware,

if the ancillary BIOS package is present in the enhancement space,
decompressing the ancillary BIOS package, and
executing the ancillary BIOS package.

25. The ancillary BIOS processing method of claim 24, further comprising searching memory for a decompressor associated with the ancillary BIOS package and, if the decompressor is not found, executing a second ancillary BIOS package from a default space of firmware.

26. A video BIOS processing method, comprising:

determining whether a video BIOS exists in an alterable firmware section of a memory system,

if no video BIOS exist in the alterable section, executing a video BIOS in a nonalterable firmware section in the memory system.

27. The method of claim 26, wherein the determining and executing steps are performed during execution of a system BIOS.

28. The method of claim 26, further comprising, if a video BIOS exists in the alterable section, executing the video BIOS in the alterable section.

29. The method of claim 26, further comprising, determining whether a predetermined user command has been entered and, if no predetermined user command has been entered, executing a video BIOS from the alterable section.

30. The method of claim 26, further comprising:
decompressing a video BIOS from the alterable section and
executing the decompressed video BIOS.
31. A video BIOS processing method, comprising:
determining whether a video BIOS package is present in an enhancement space of
firmware,
if the video BIOS package is present, determining whether a predetermined user
command has been entered,
if the predetermined user command has not been entered, executing the video
BIOS package from the enhancement space,
otherwise, executing a video BIOS from a default space of firmware.
32. The method of claim 31, further comprising:
decompressing a video BIOS from the alterable section and
executing the decompressed video BIOS.
33. A video BIOS processing method, comprising:
determining whether a video BIOS package is present in an enhancement space of
firmware,
if the video BIOS package is present, determining whether a predetermined flag
has been set in the firmware,
if the predetermined user command has been set, executing the video BIOS
package from the enhancement space,
otherwise, executing a video BIOS from a default space of firmware.
34. The method of claim 34, further comprising:
decompressing a video BIOS from the alterable section and
executing the decompressed video BIOS.
35. A video BIOS processing method, comprising:
determining whether a video BIOS package is present in an enhancement space of
firmware,

if the video BIOS package is present in the enhancement space, decompressing the video BIOS package, and
executing the video BIOS package.

36. The video BIOS processing method of claim 35, further comprising searching memory for a decompressor for the video BIOS package and if the decompressor is not found executing a second video BIOS package from a default space of firmware.

37. A computer readable medium having stored there on program instructions that, when executed by a processor, cause the processor to:

receive a data object having a BIOS package and an associated signature,

authenticate the BIOS package using a public key stored on the computer and the signature, and

if the authentication succeeds, write the BIOS package to firmware on the computer system.

38. The medium of claim 37, wherein the signature is generated by a public key-private key pair, the public key of which may be read by the processor from a memory.

39. The medium of claim 37, wherein the receiving comprises load the data object from a storage device.

40. The medium of claim 37, wherein the receiving comprises receiving the data object from a communication network.

41. The medium of claim 37, wherein the receiving comprises receiving the data object from a computer network.

42. The medium of claim 37, further comprising, prior to the write:

via an operating system, store fragments of the received data object in system memory,

create a table identifying locations of each fragment in system memory, and
assemble the BIOS package from the fragments using the table.